CLAIMS

WHAT IS CLAIMED IS:

1. A method for detecting intrusions on a network, comprising:

storing signature profiles identifying patterns associated with network intrusions in a signature database;

generating classification rules based on said signature profiles;

receiving data packets transmitted on the network;

classifying data packets having corresponding classification rules according to said generated classification rules; and

forwarding said classified packets to a signature engine for comparison with signature profiles.

2. The method of claim 1 further comprising dropping data packets without corresponding classification rules.

3. The method of claim 1 wherein classifying said packets comprises classifying said packets according to at least one packet field into groups.

4. The method of claim 3 further comprising classifying said packets within each of the groups according to packet type or size.

5. The method of claim 4 wherein classifying said packets according to packet size or type comprises classifying said packets according to TCP flags.

6. The method of claim 4 wherein classifying said packets according to packet size or type comprises classifying said packets according to packet length.

7. The method of claim 3 wherein classifying said packets according to at least one packet field comprises classifying said packets according to protocol type.

8. The method of claim 3 wherein classifying said packets according to at least one packet field comprises classifying said packets according to destination port number.

9. The method of claim 3 wherein classifying said packets according to at least one packet field comprises classifying said packets according to destination address.

10. The method of claim 1 further comprising performing a table lookup to select an action to be performed on said packet based on its classification.

11. The method of claim 10 wherein one of the actions is comparing said packet to at least a subset of the signature profiles.

12. The method of claim 10 wherein one of the actions of the table is dropping the packet.

13. The method of claim 10 further comprising generating an alert following the table lookup.

14. The method of claim 10 wherein the lookup is performed in a flow table and further comprising updating a field of the flow table.

15. The method of claim 1 further comprising partitioning signatures into disjoint groups to define subsets of signature profiles.

16. The method of claim 15 further comprising comparing said packets to at least one of the subsets of signature profiles.

17. The method of claim 1 further comprising filtering said received packets.

18. The method of claim 1 wherein receiving said packets comprises capturing said packets at a network analysis device.

19. The method of claim 18 further comprising decoding protocols after receiving said packets.

20. An intrusion detection system comprising:

a signature classifier comprising a first stage classifier operable to classify packets according to at least one packet field into groups and a second stage classifier operable to classify said packets within each of the groups according to packet type or size;

a flow table configured to support table lookups of actions associated with classified packets;

a signature database for storing signature profiles identifying patterns associated with network intrusions; and

a detection engine operable to perform a table lookup at the flow table to select an action to be performed on said packet based on its classification, wherein comparing said packets to at least a subset of the signature profiles is one of the actions.

21. The system of claim 20 further comprising a data monitoring device having a capture engine operable to capture data passing through the network and configured to monitor network traffic, decode protocols, and analyze received data.

22. The system of claim 21 further comprising application program interfaces configured to allow the intrusion detection system access to applications of the data monitoring device to perform intrusion detection; and

23. The system of claim 21 further comprising a parser operable to parse, generate, and load signatures at the detection engine.

24. The system of claim 21 further comprising an alarm manager operable to generate alarms.

25. The system of claim 21 further comprising a filter configured to filter out packets received at the intrusion detection system.

26. The system of claim 21 further comprising a capture engine configured to forward packets and temporarily store packets for later analysis by the data monitoring device.

27. The system of claim 20 wherein the flow table is a hash table.

28. The system of claim 20 wherein action options listed in the flow table include dropping the packet and generating an alarm.

29. The system of claim 28 wherein action options further include dropping the packet and updating one or more fields of the flow table.

30. A computer program product for detecting intrusions on a network, comprising:

code that stores signature profiles identifying patterns associated with network intrusions in a signature database;

code that generates classification rules based on said signature profiles;

code that receives data packets transmitted on the network;

code that classifies data packets having corresponding classification rules according to said generated classification rules;

code that forwards said classified packets to a signature engine for comparison with signature profiles and stores signature profiles identifying patterns associated with network intrusions in a signature database; and

a computer-readable storage medium for storing the codes.